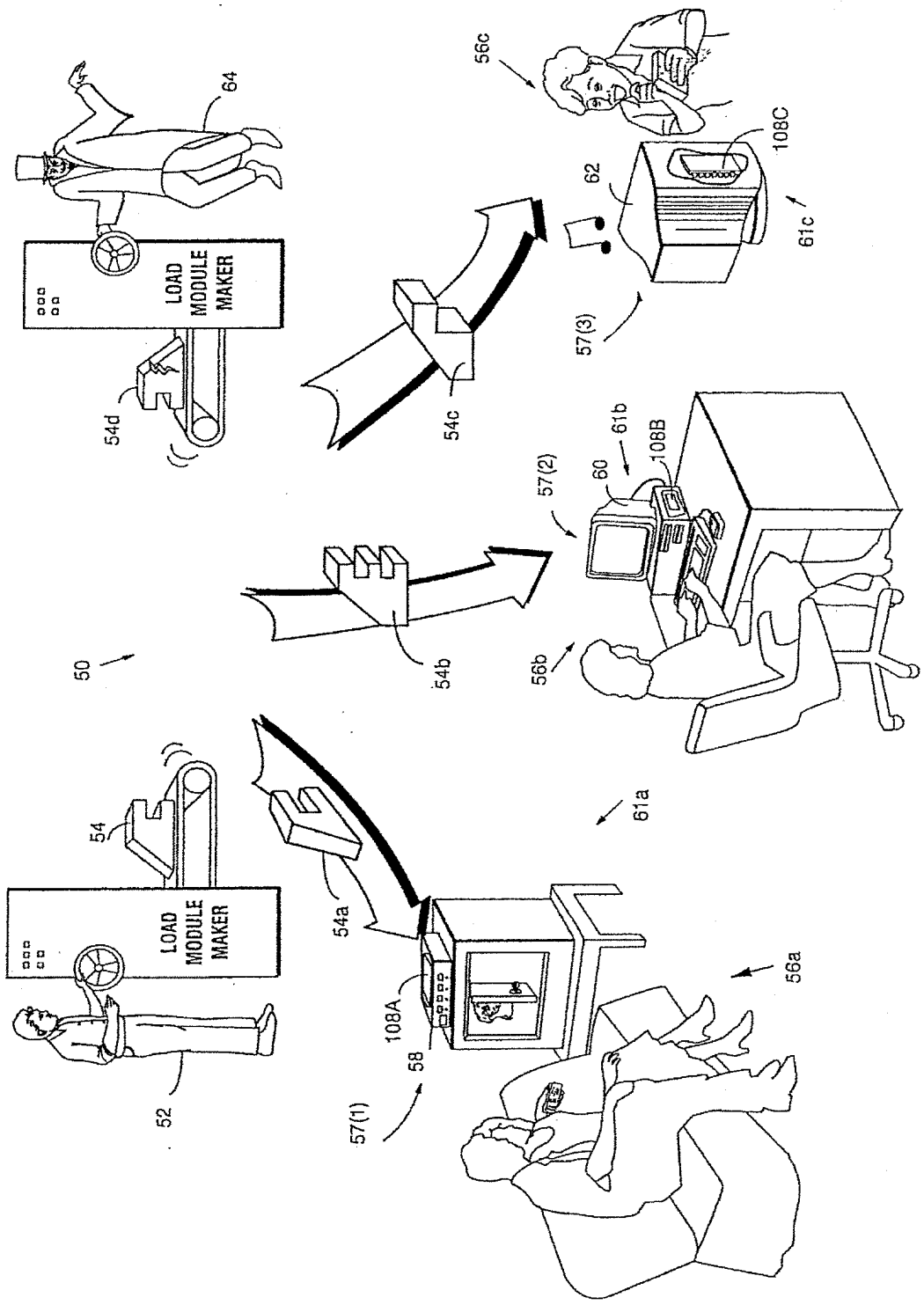


FIG. 1 Defective or "Bogus" Load Modules Can Cause Problems

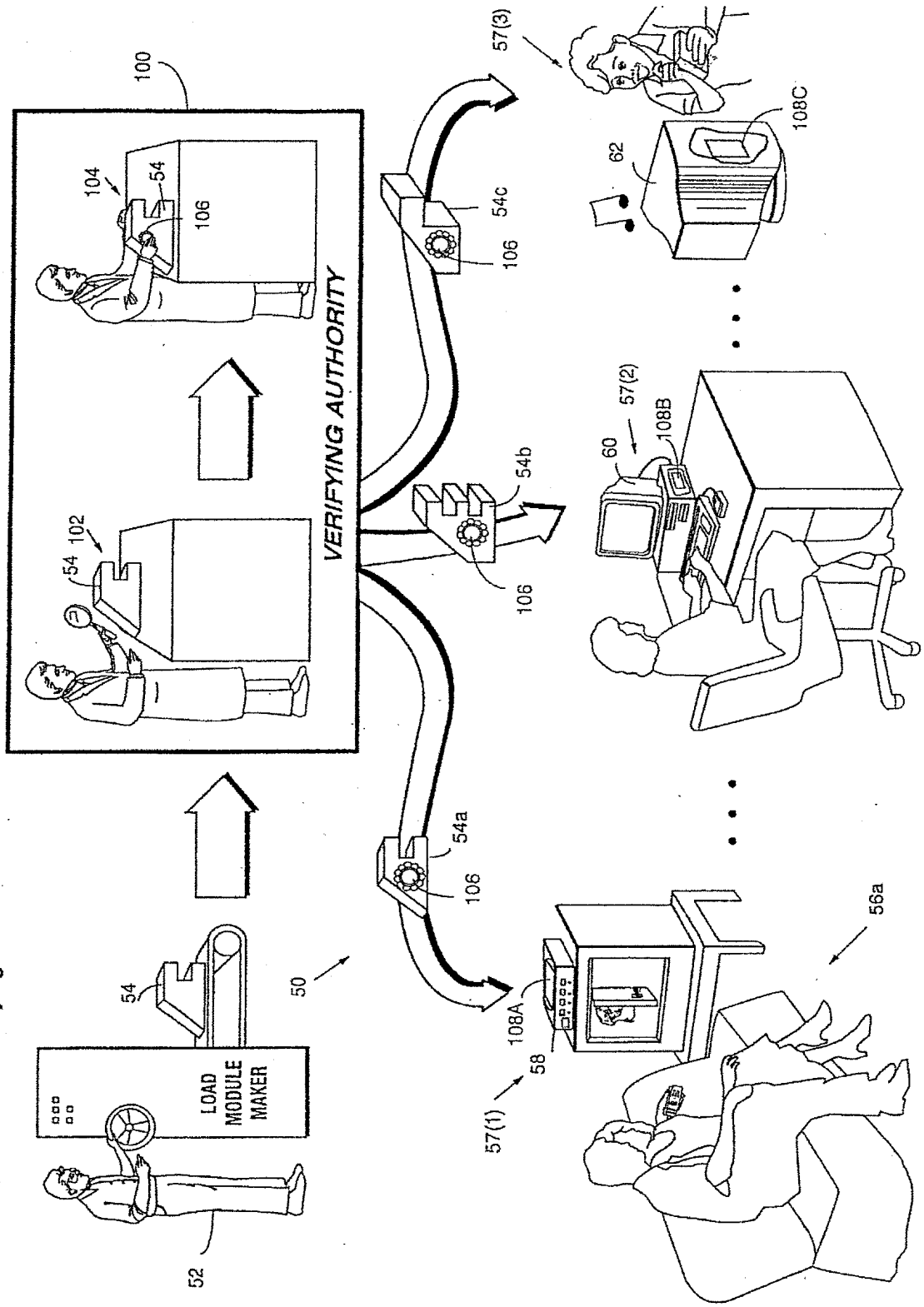


FIG. 2 Verifying Load Modules

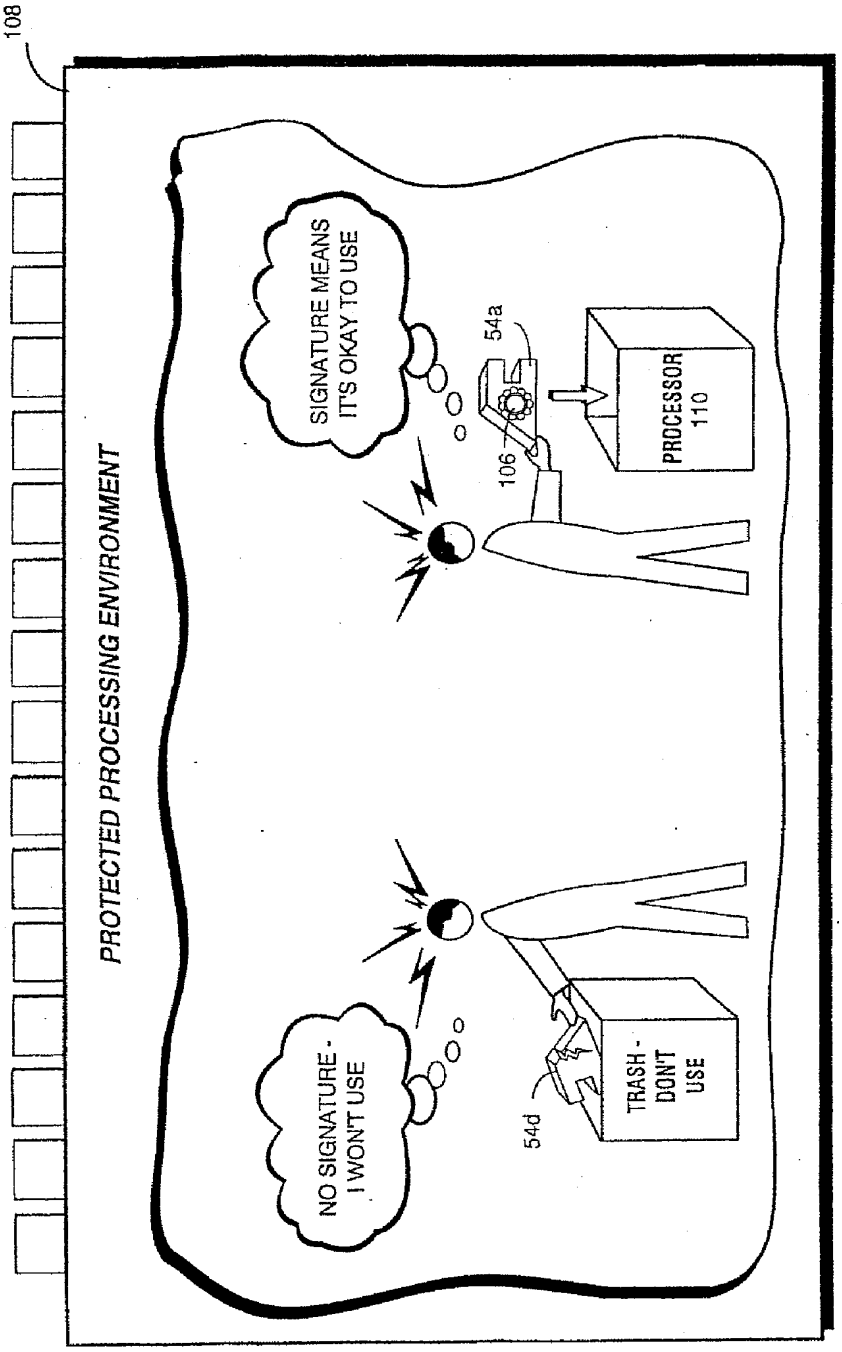


FIG. 3 Before Protected Processing Environment Uses A Load Module, It Checks To See If Load Module Has Been Verified

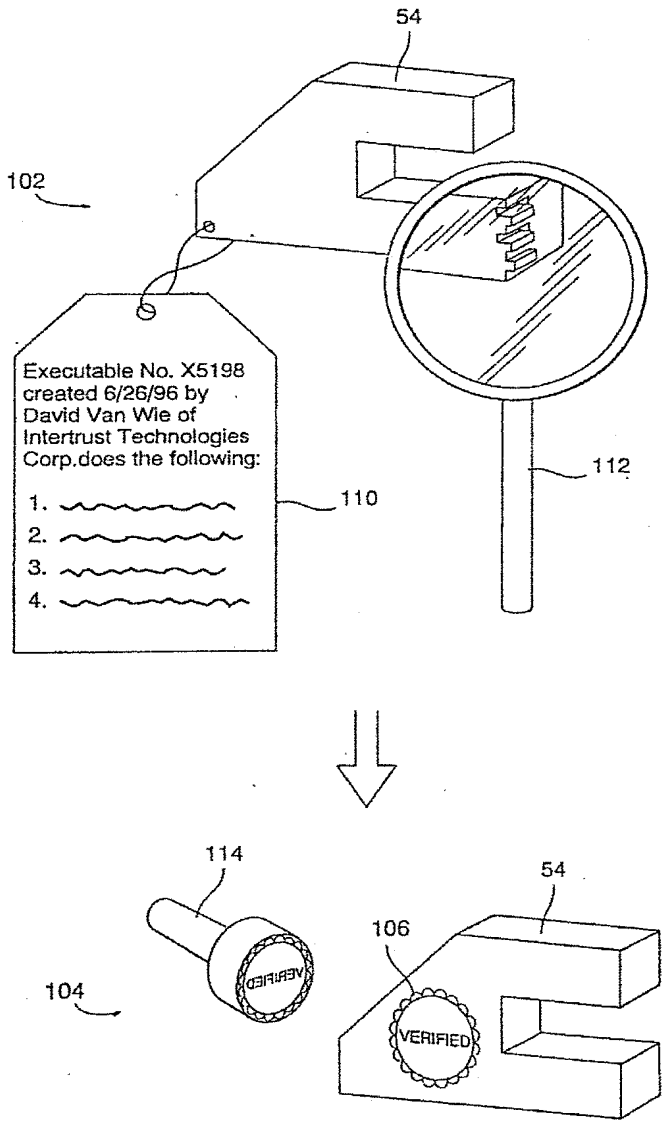


FIG. 4

Certifying Load Module by
Checking it Against its Documentation

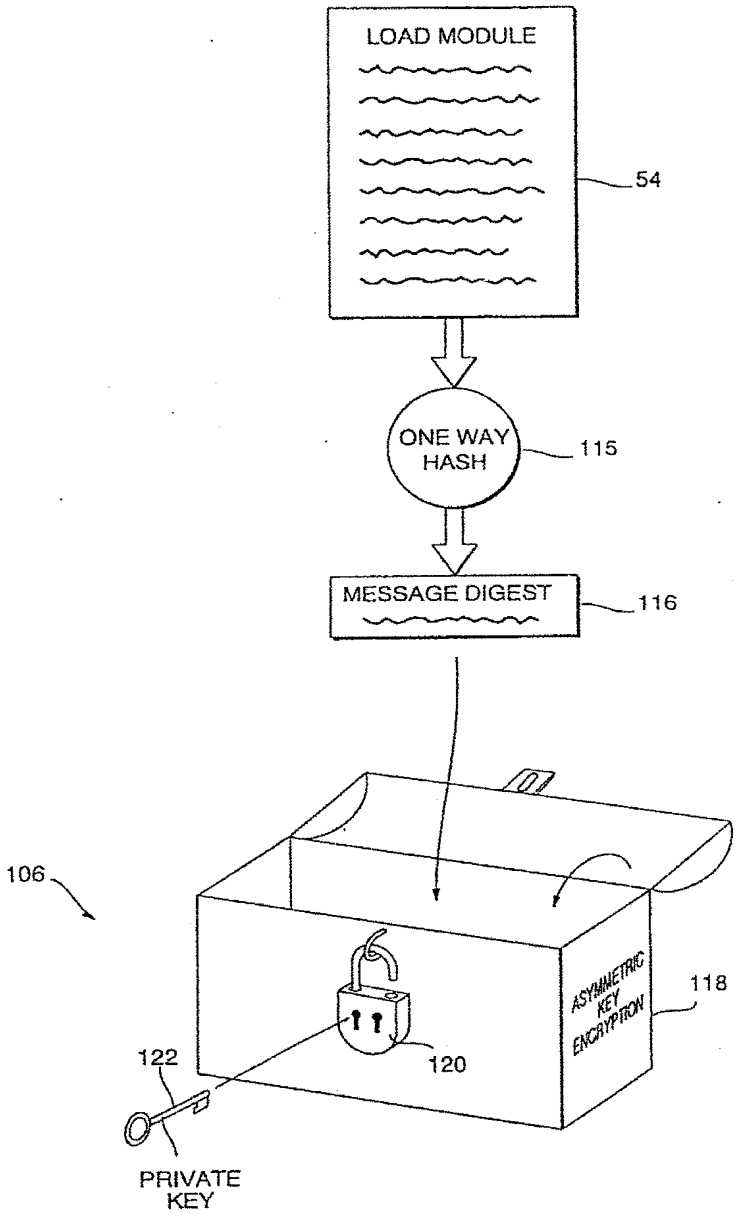


FIG. 5

Creating a Certifying Digital Signature

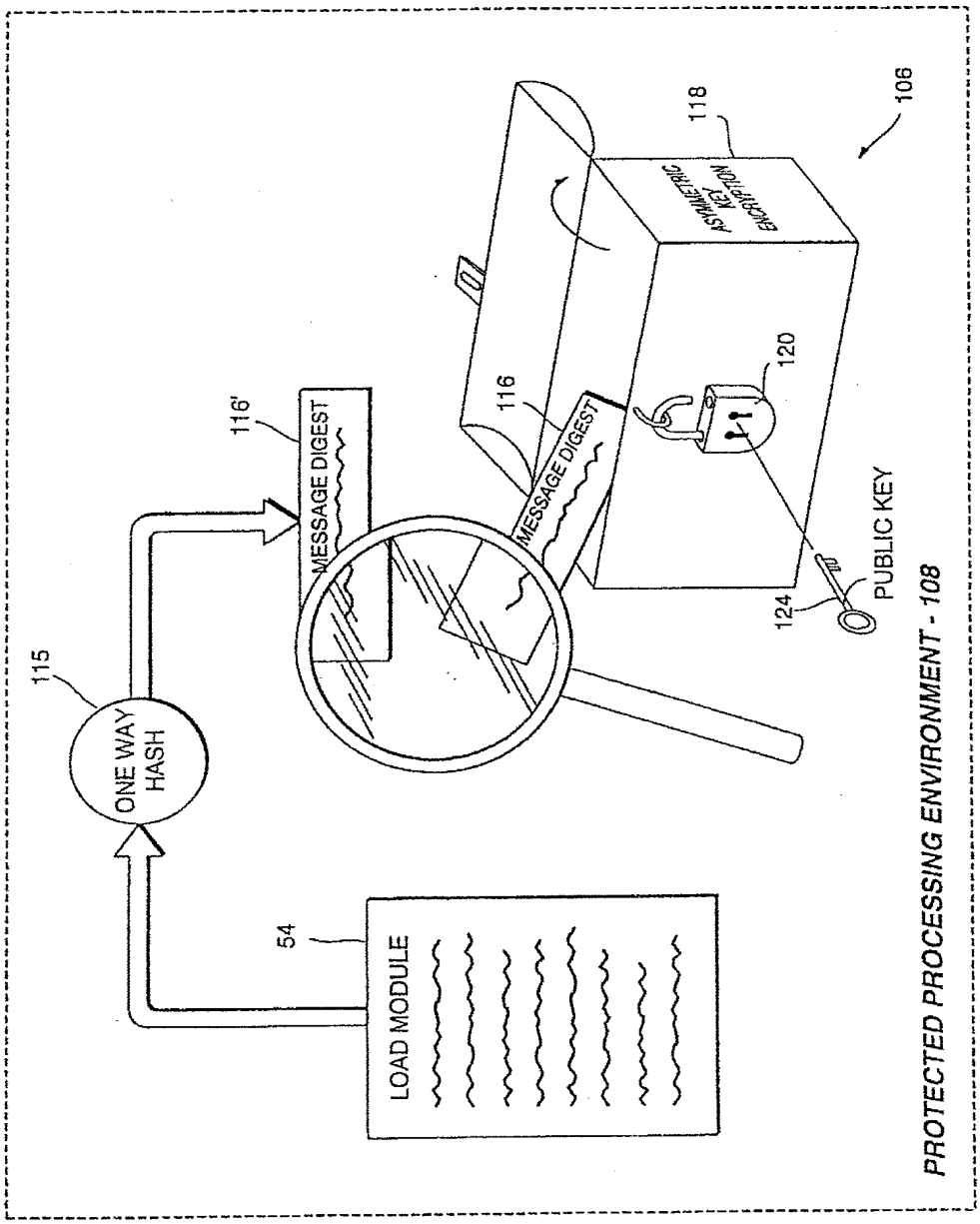


FIG. 6 Authenticating a Digital Signature

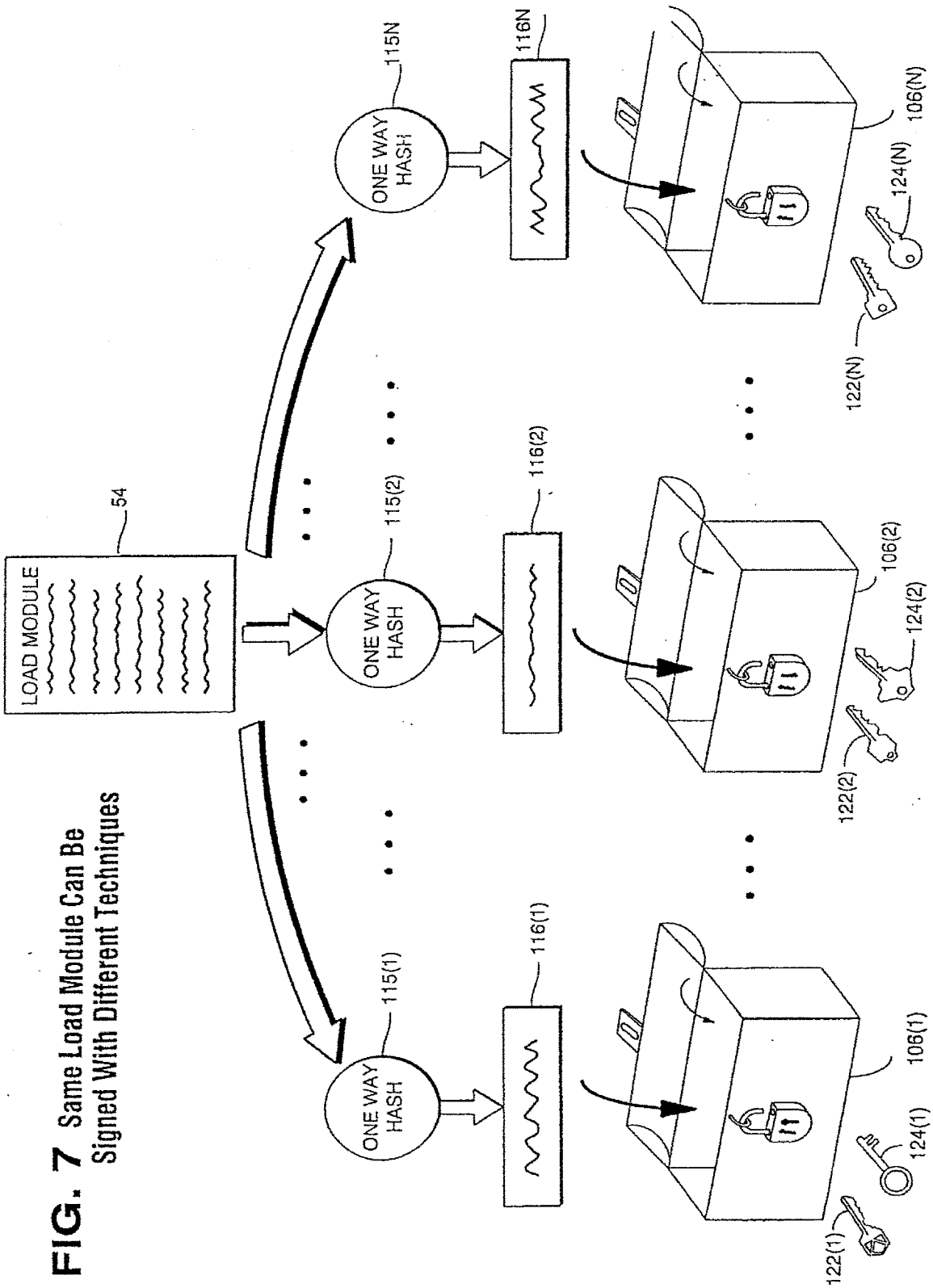


FIG. 7 Same Load Module Can Be Signed With Different Techniques

FIG. 8 Same Load Module Can Be Distributed with Multiple Signatures

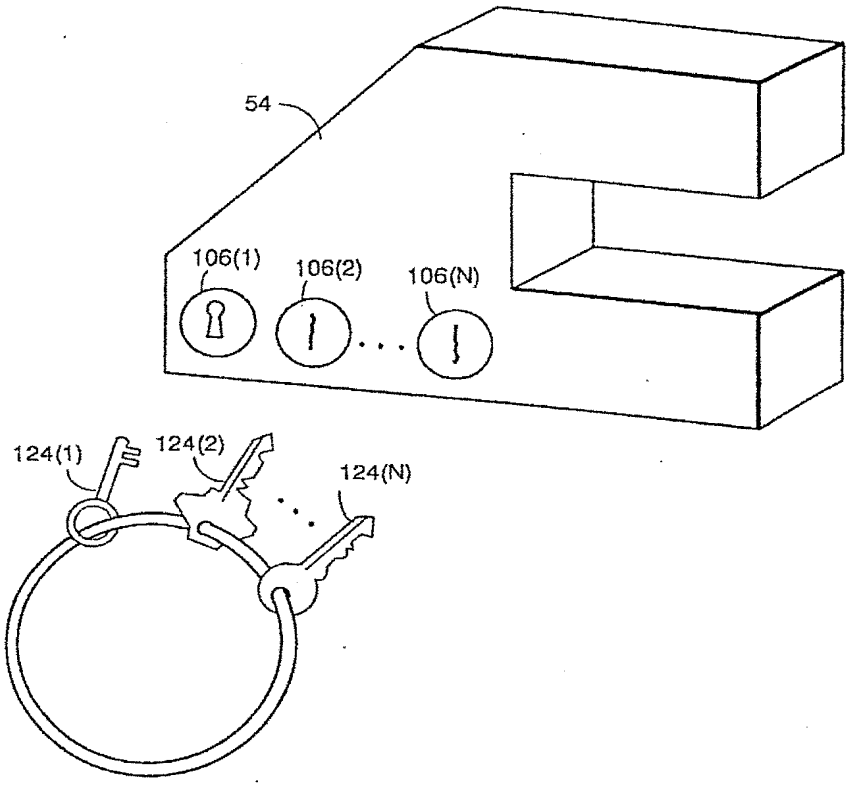


FIG. 8A Different Processing Environments Can Have Different Subsets of Keys

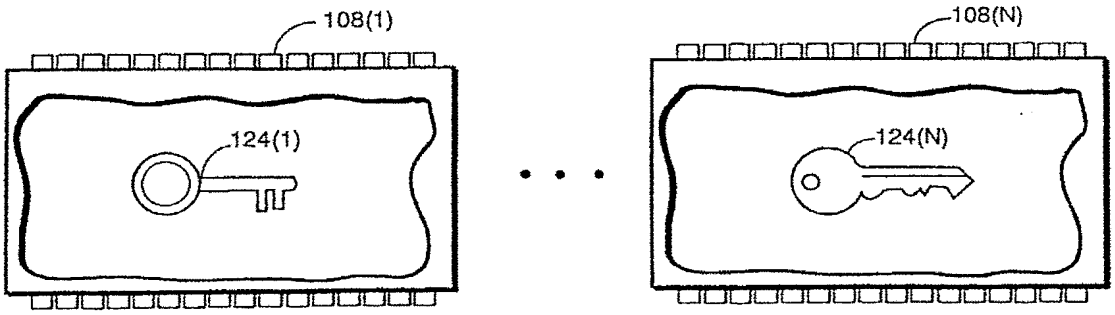
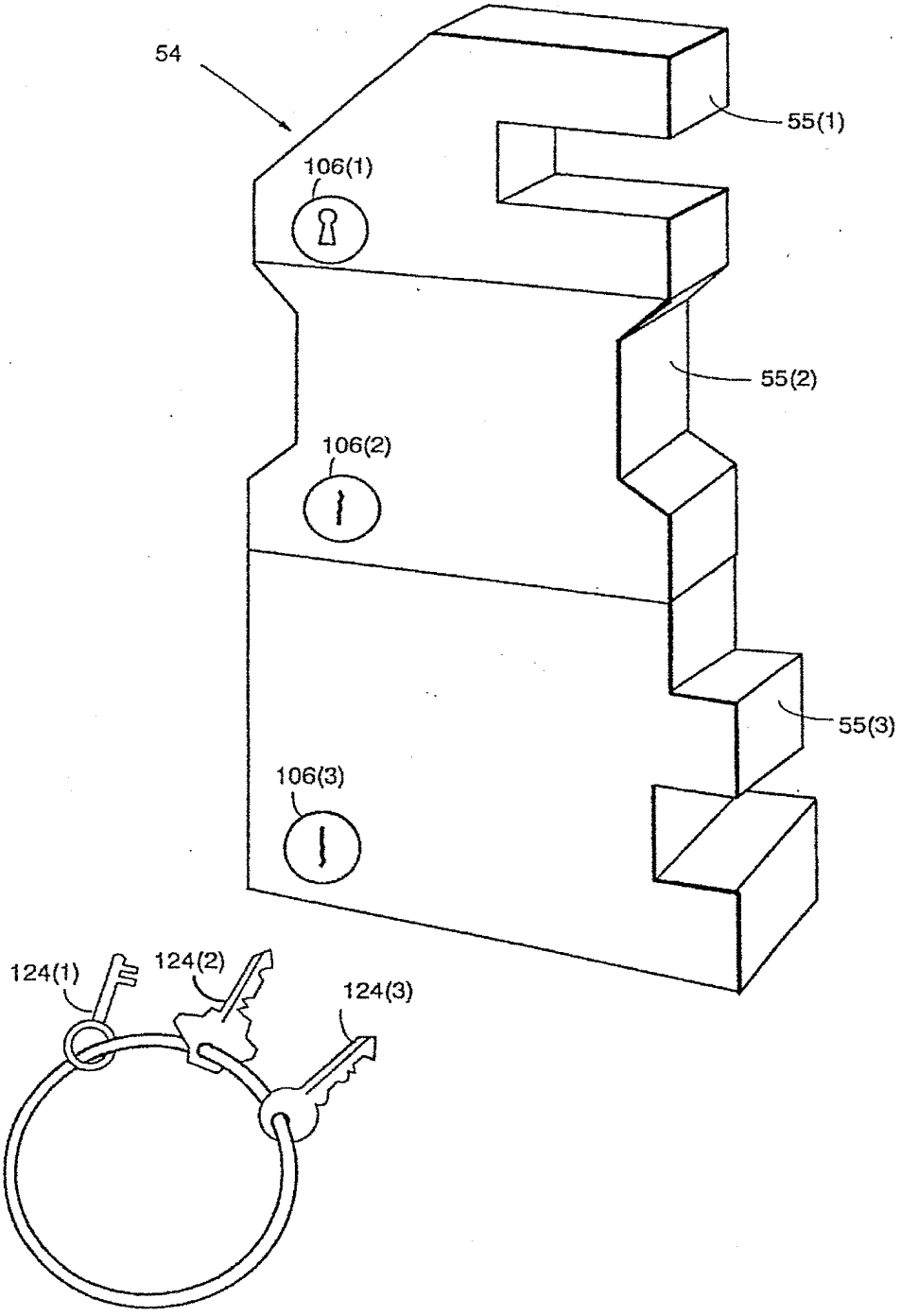


FIG. 9 Load Module Can Have Several Independently Signed Portions



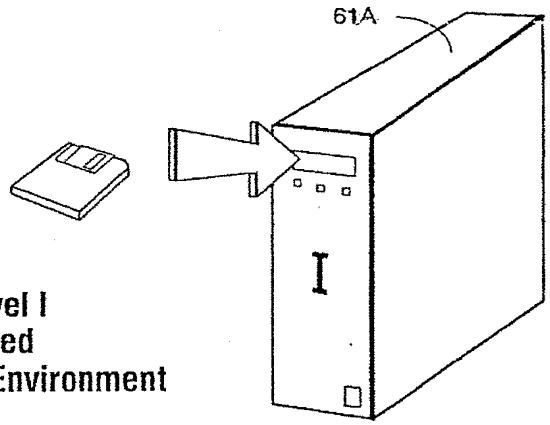


FIG. 10A Assurance Level I
Software-Based
Protected Processing Environment

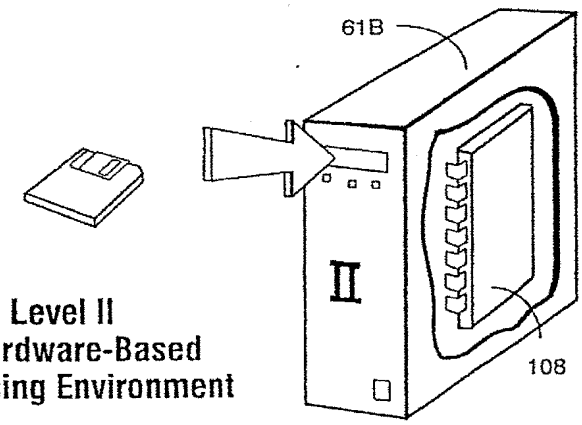


FIG. 10B Assurance Level II
Software and Hardware-Based
Protected Processing Environment

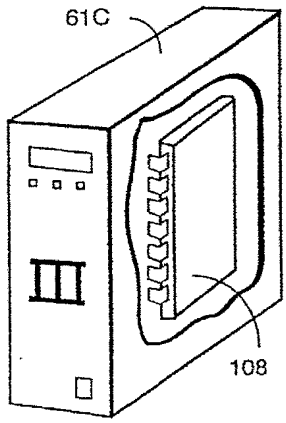


FIG. 10C Assurance Level III
Hardware-Based
Protected Processing Environment

FIG. 11A Level I
Digital Signature

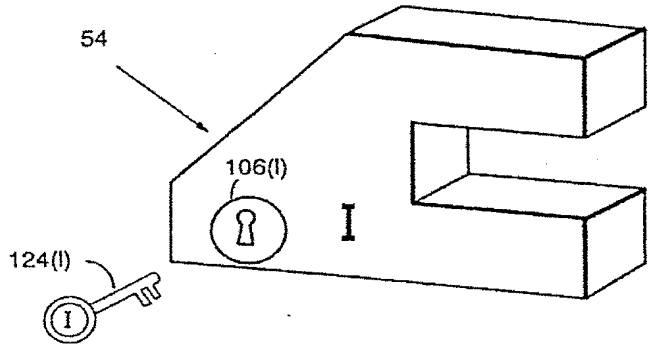


FIG. 11B Level II
Digital Signature

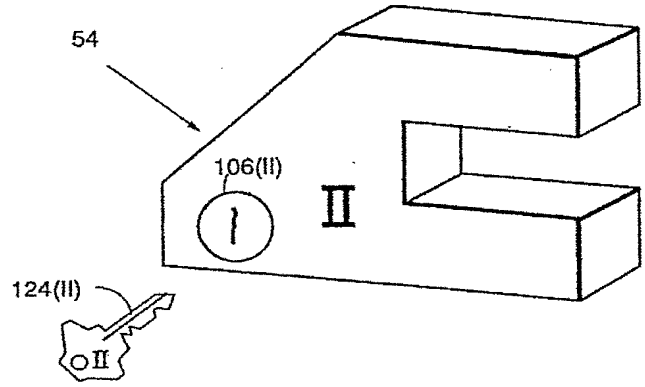
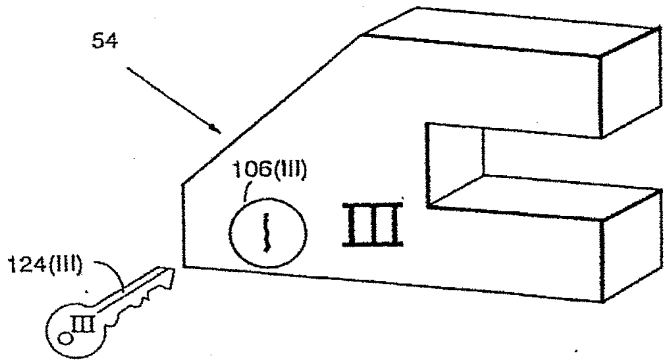


FIG. 11C Level III
Digital Signature



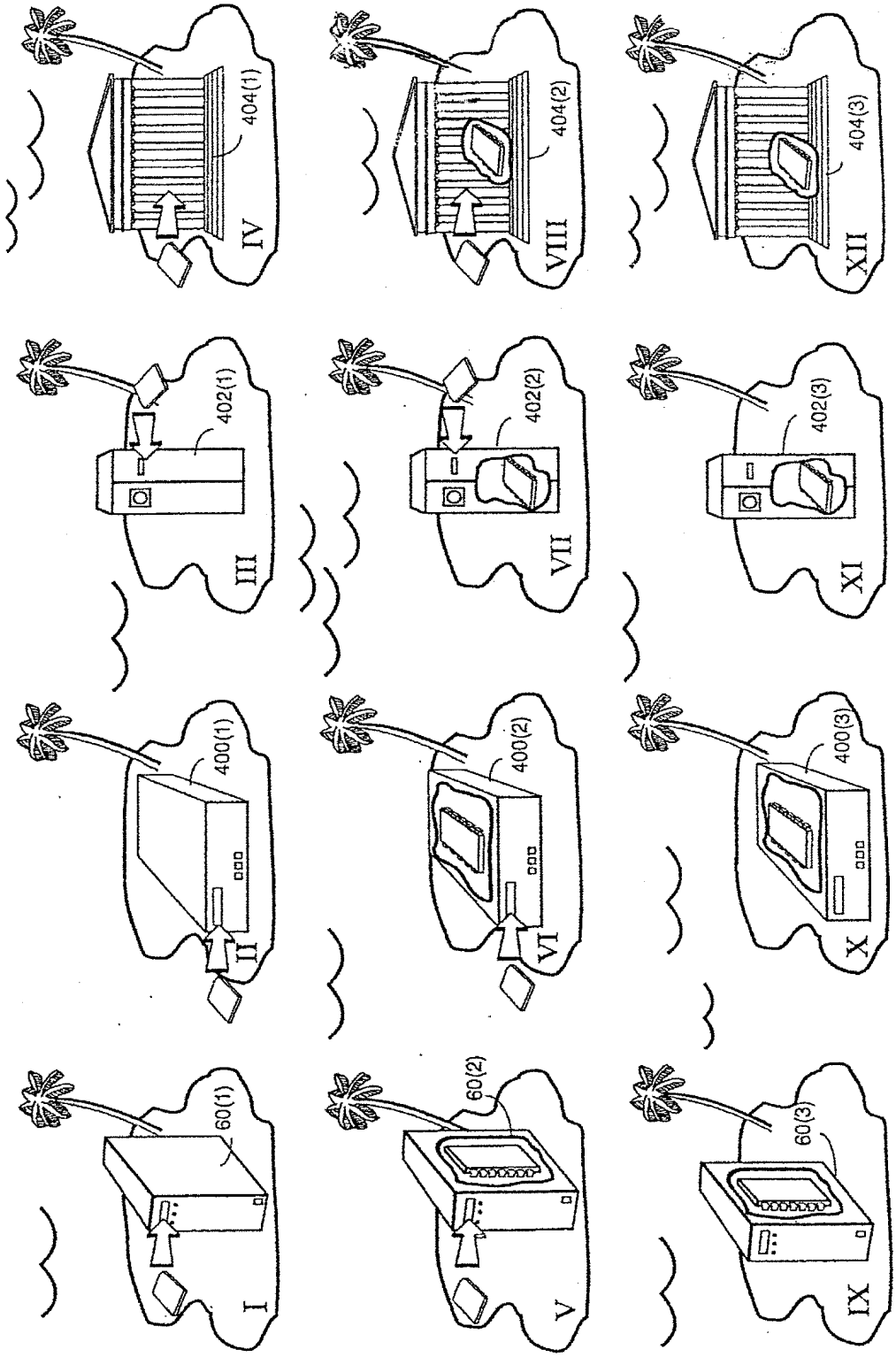


FIG. 12 Using Digital Signatures For Compartmentalizing Different Assurance Levels

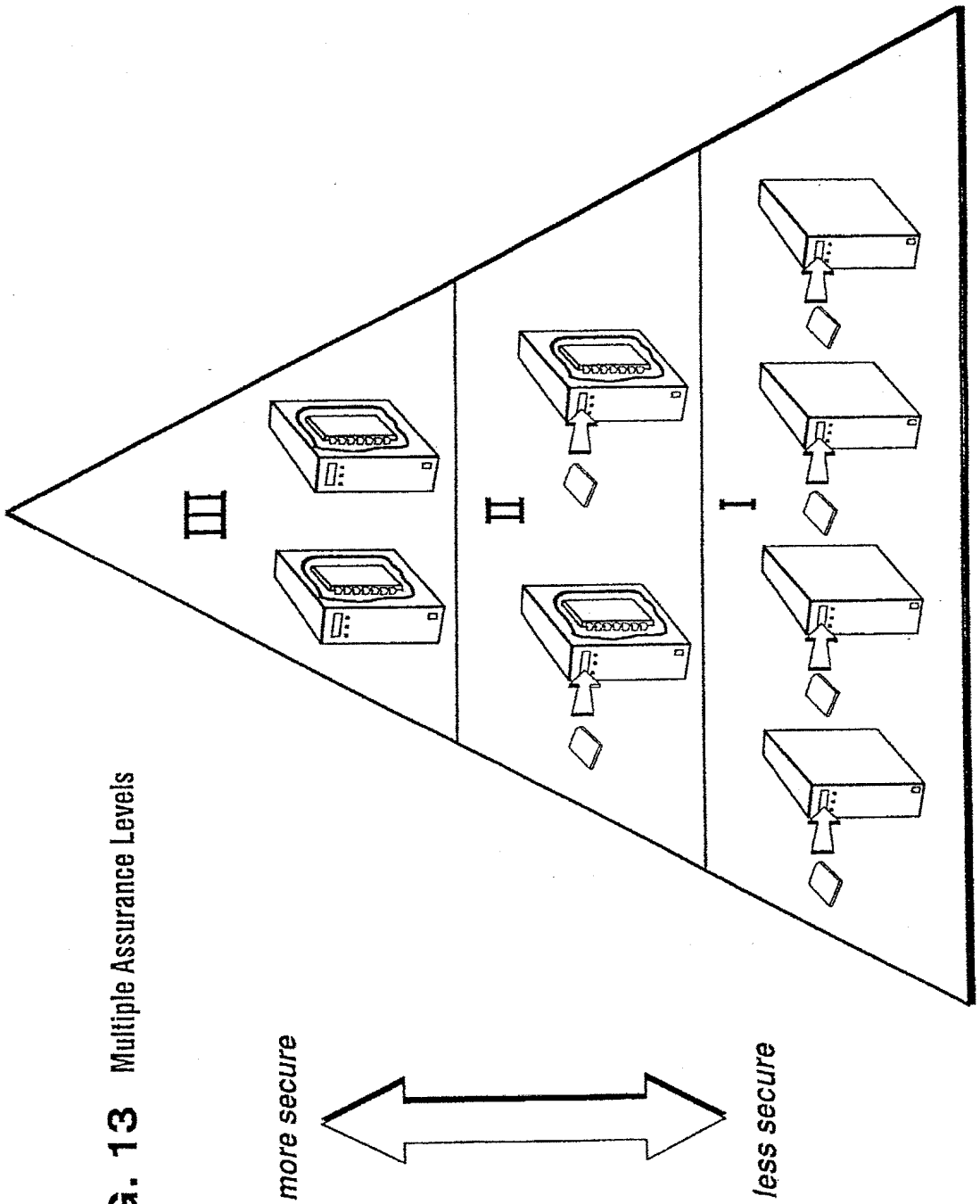


FIG. 13 Multiple Assurance Levels

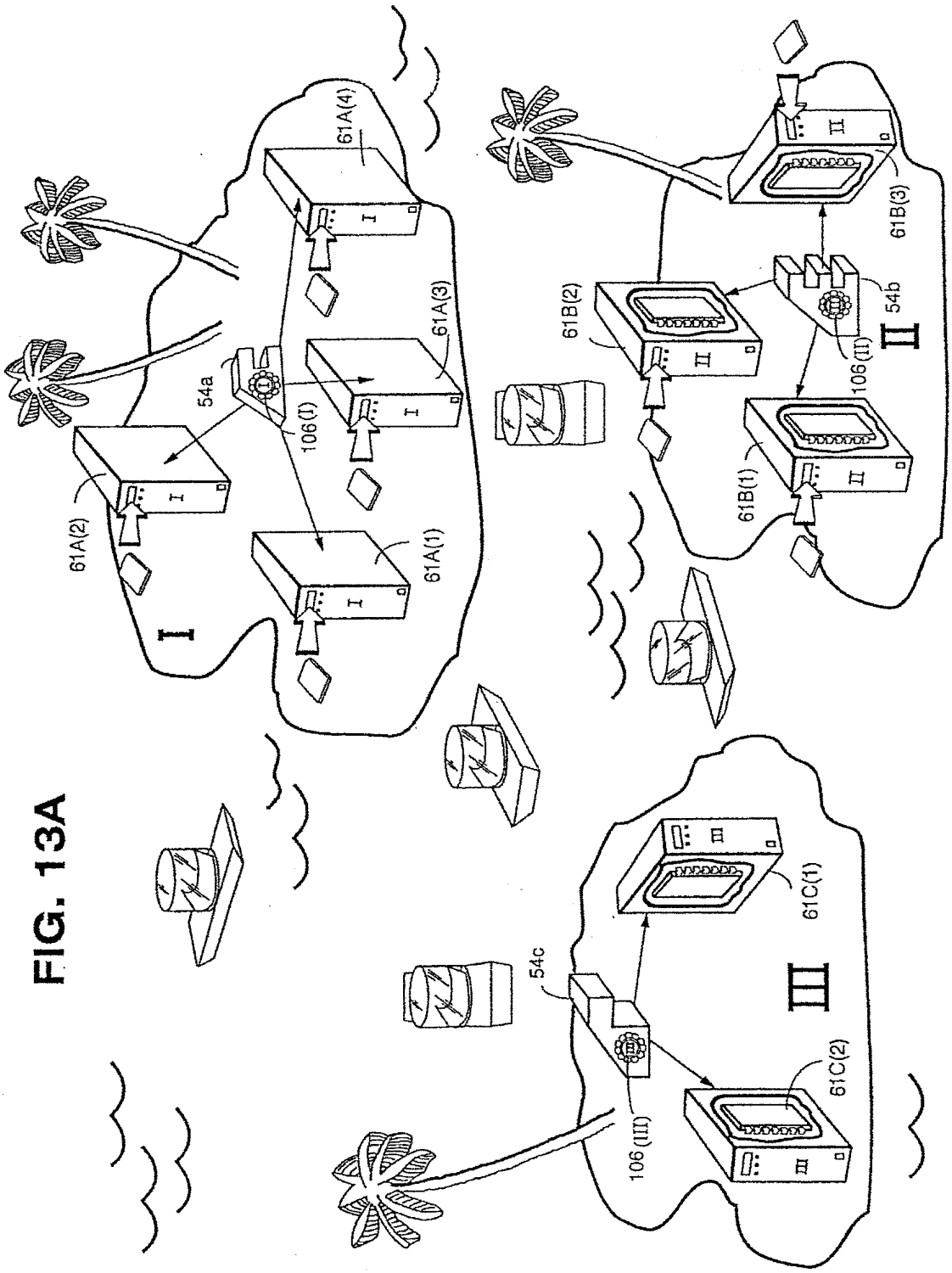
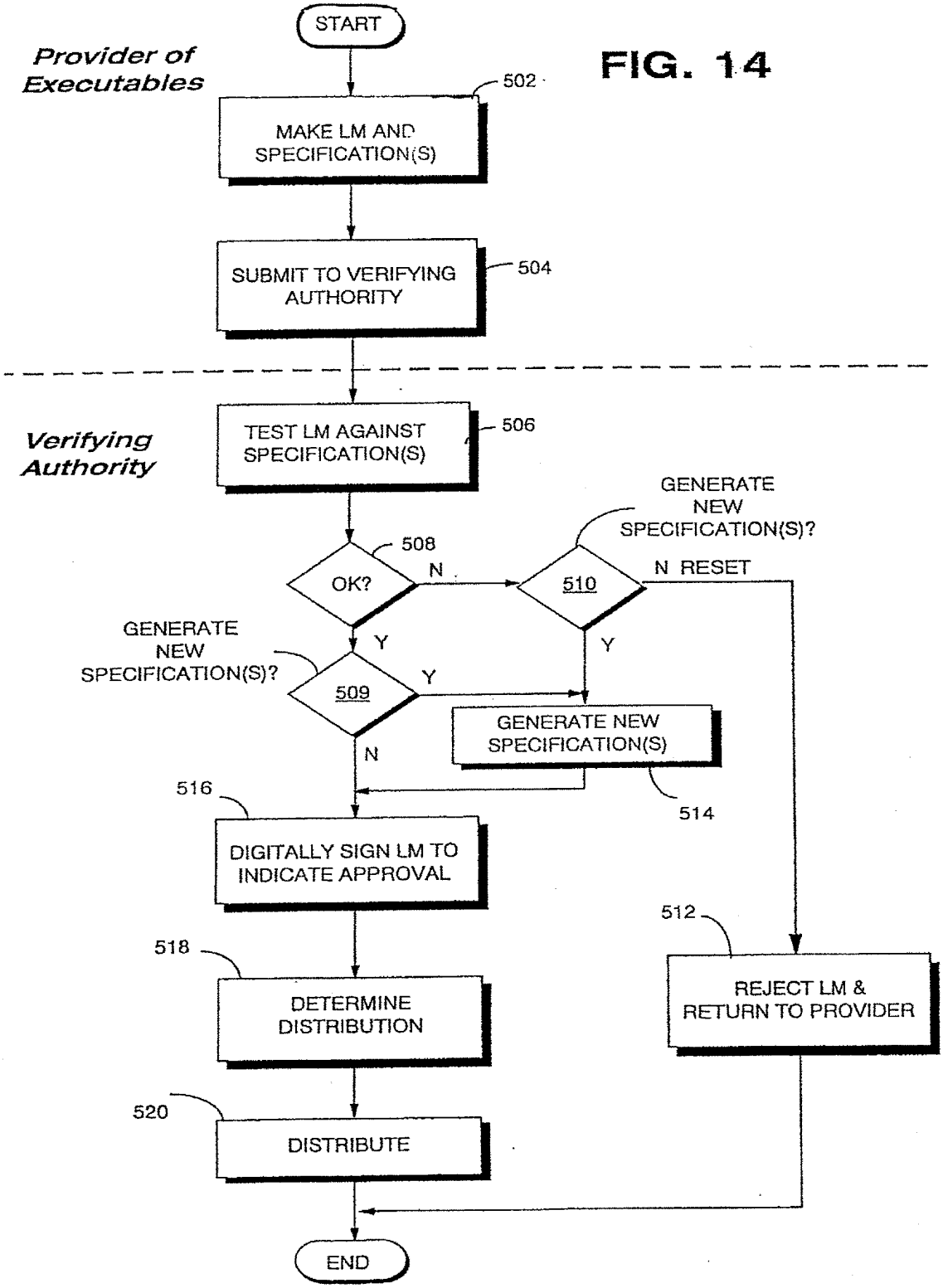

61A(4)
61A(3)
54a
106(I)
61A(2)
61A(1)
I
61B(3)
61B(2)
54b
106(II)
II
61B(1)
61C(1)
54c
III
106 (III)
61C(2)

FIG. 13A

FIG. 14


Provider of Executables
START
502
MAKE LM AND SPECIFICATION(S)
SUBMIT TO VERIFYING AUTHORITY
504
Verifying Authority
TEST LM AGAINST SPECIFICATION(S)
506
508
OK?
N
GENERATE NEW SPECIFICATION(S)?
510
N RESET
Y
Y
GENERATE NEW SPECIFICATION(S)?
509
Y
GENERATE NEW SPECIFICATION(S)
N
514
516
DIGITALLY SIGN LM TO INDICATE APPROVAL
512
518
DETERMINE DISTRIBUTION
REJECT LM & RETURN TO PROVIDER
520
DISTRIBUTE
END

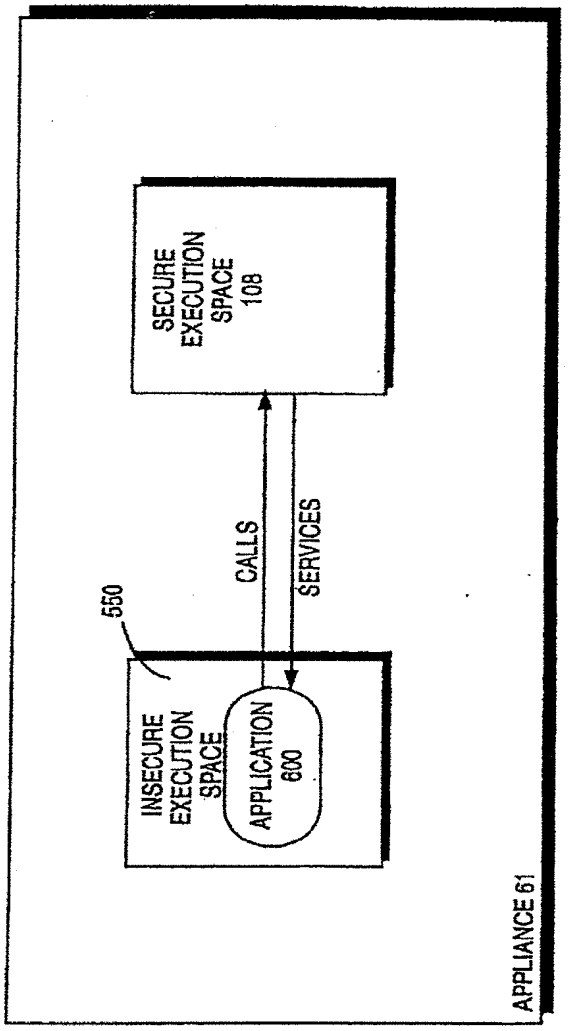


FIG. 15 EXAMPLE APPLIANCE EXECUTING APPLICATION PROGRAM IN INSECURE EXECUTION SPACE

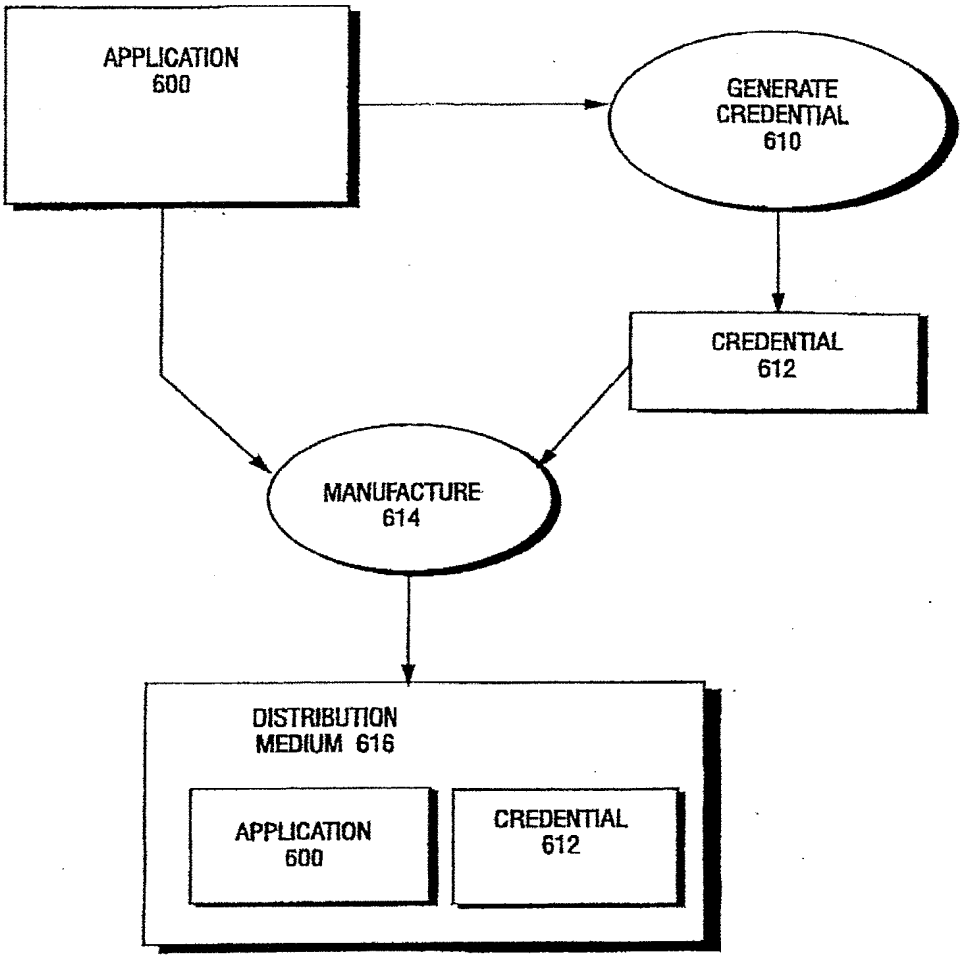


FIG. 16 EXAMPLE APPLICATION CERTIFICATION PROCESS

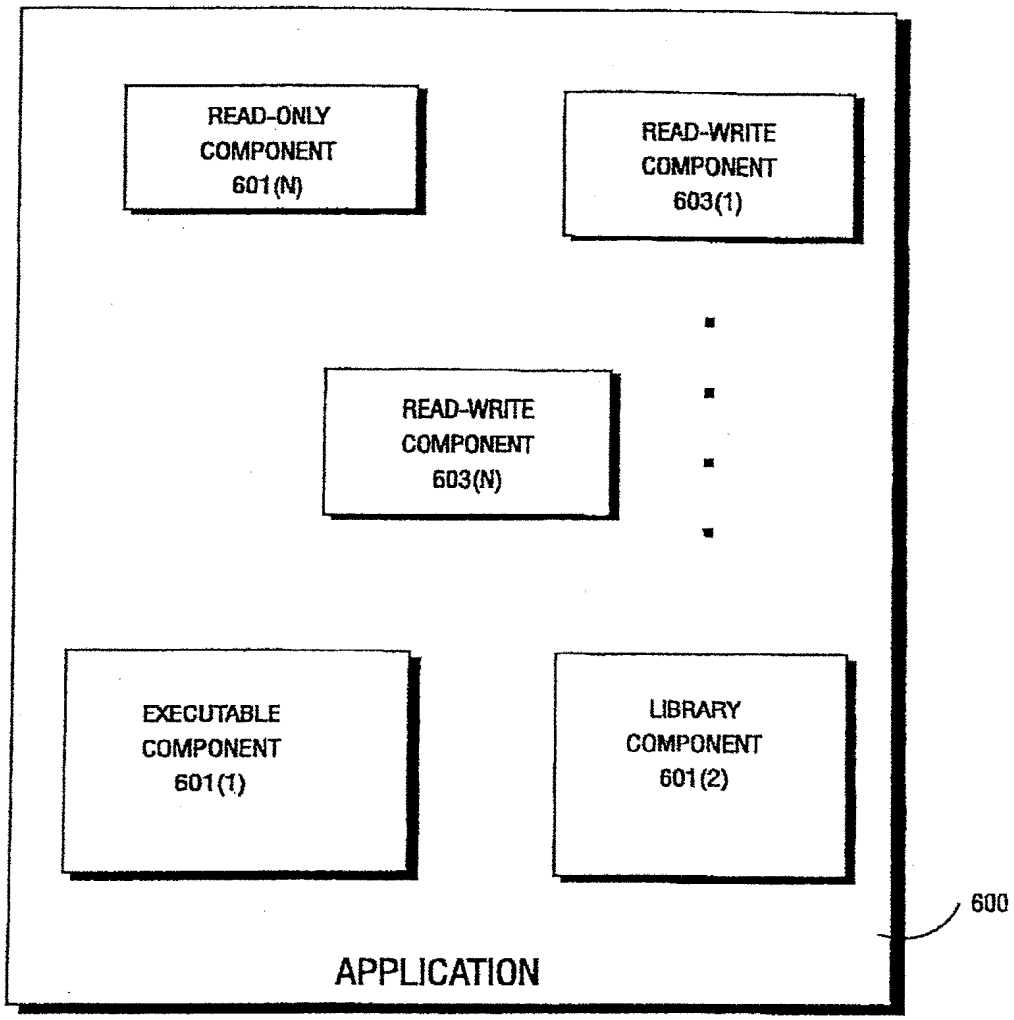


FIG. 16A EXAMPLE APPLICATION PROGRAM AND COMPONENTS

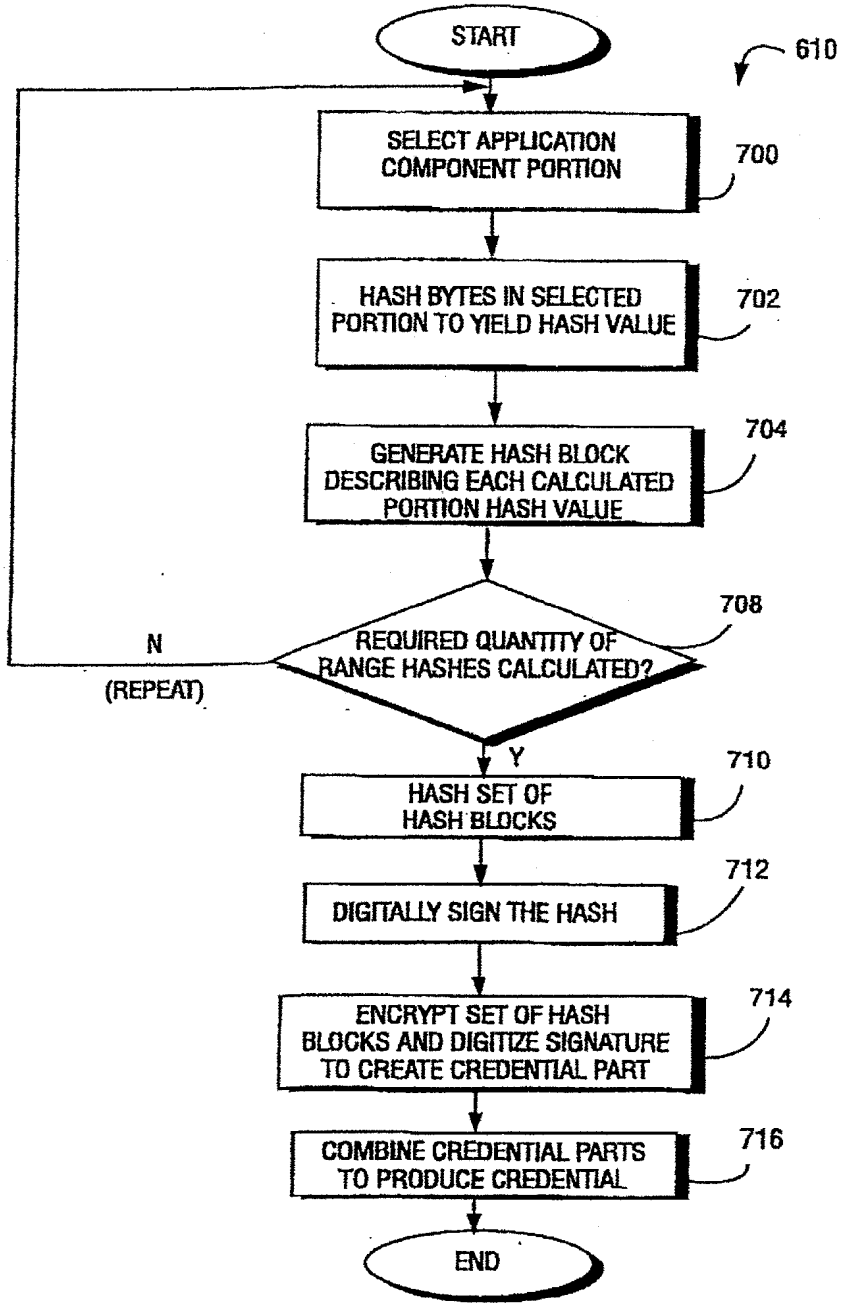


FIG. 17 EXAMPLE CREDENTIAL CREATION PROCESS

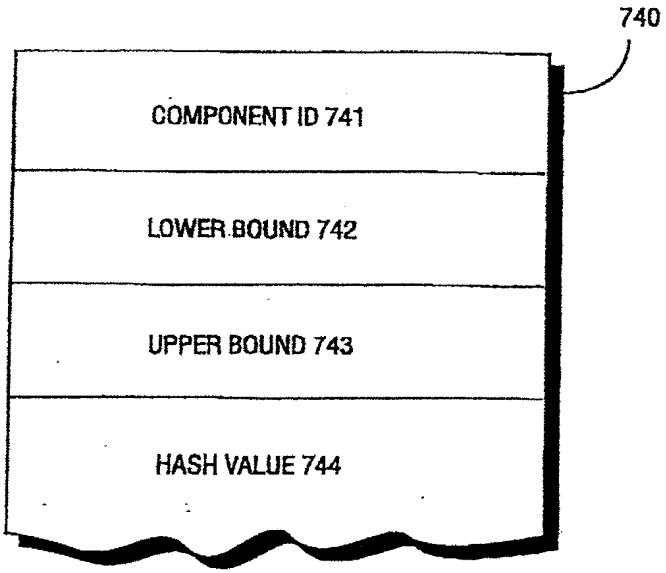


FIG. 18 EXAMPLE HASH BLOCK

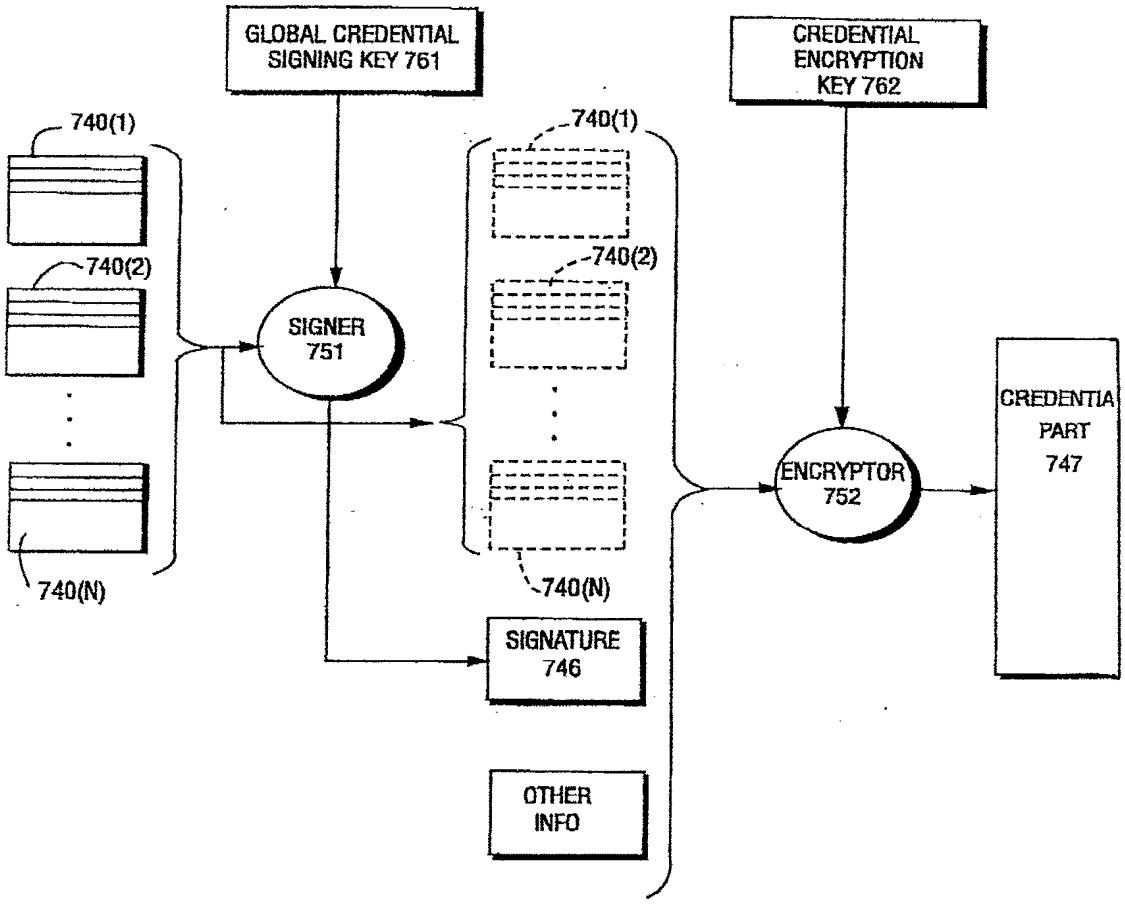


FIG. 19 EXAMPLE CREDENTIAL CREATION

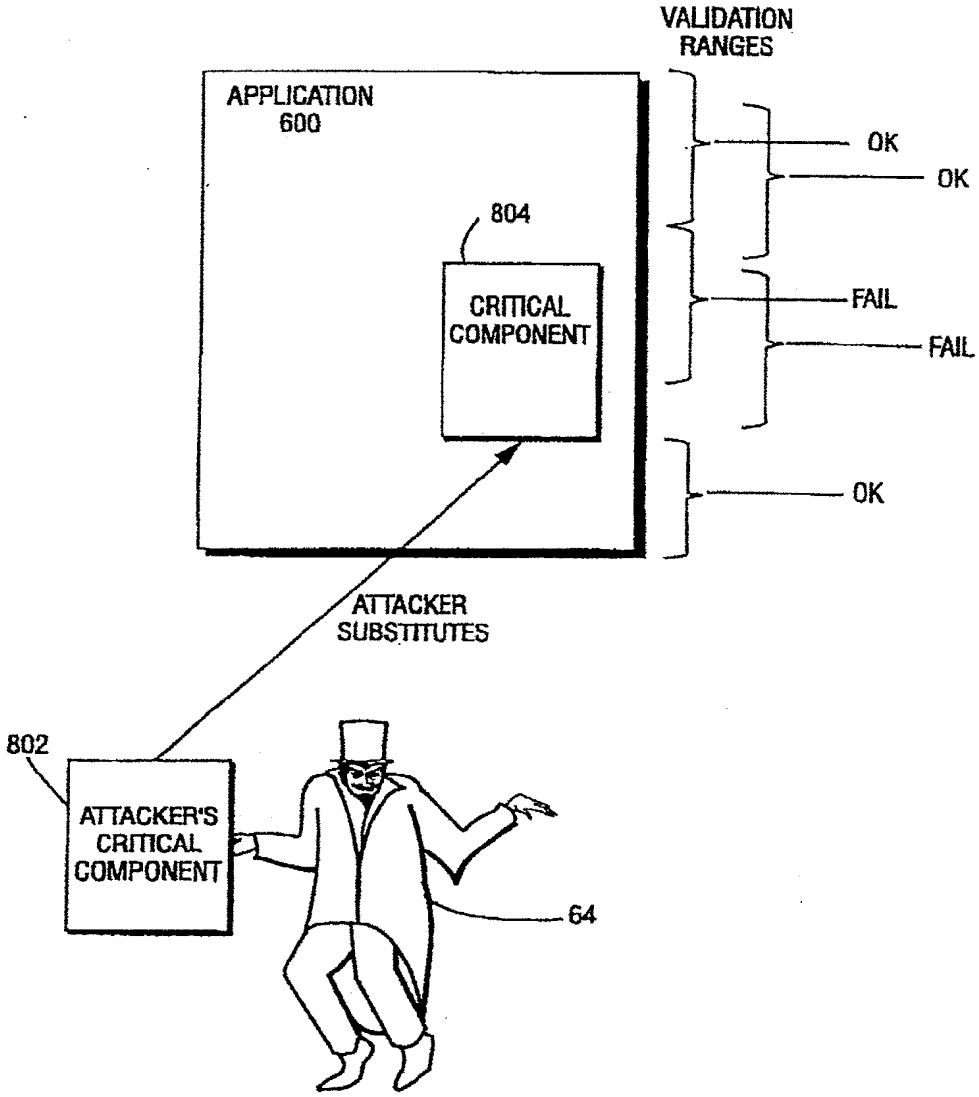


FIG. 20 EXAMPLE ATTACK ON APPLICATION

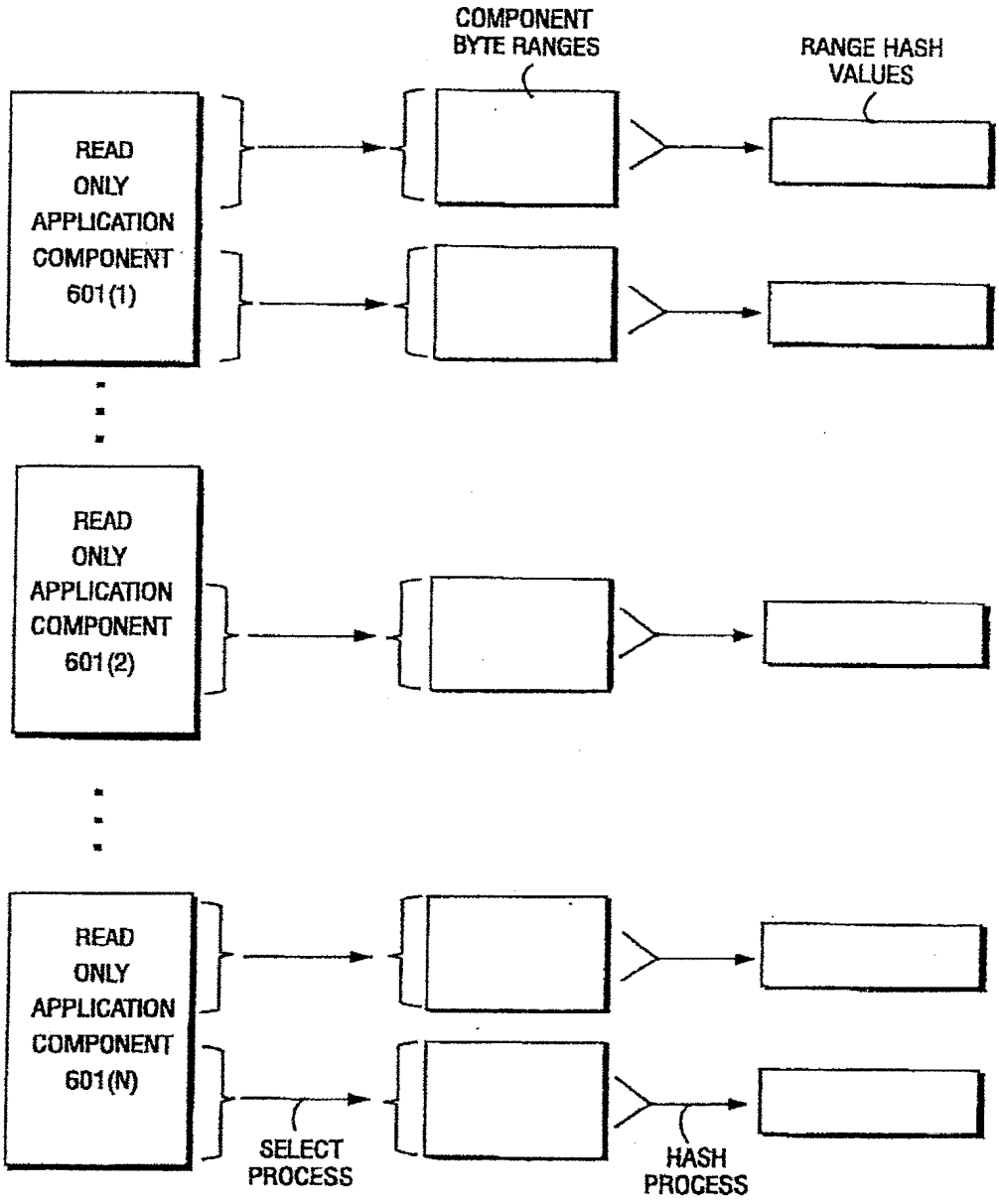


FIG. 20A EXAMPLE NON-OVERLAPPING HASH RANGES

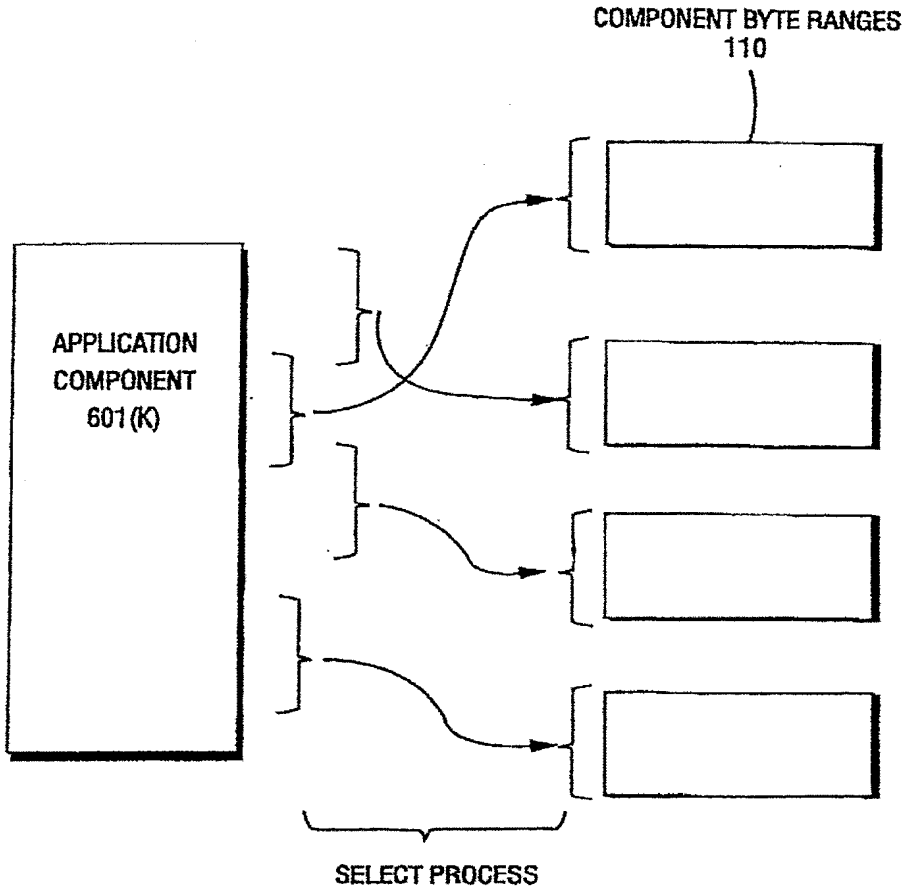


FIG. 20B EXAMPLE OF OVERLAPPING HASH RANGES

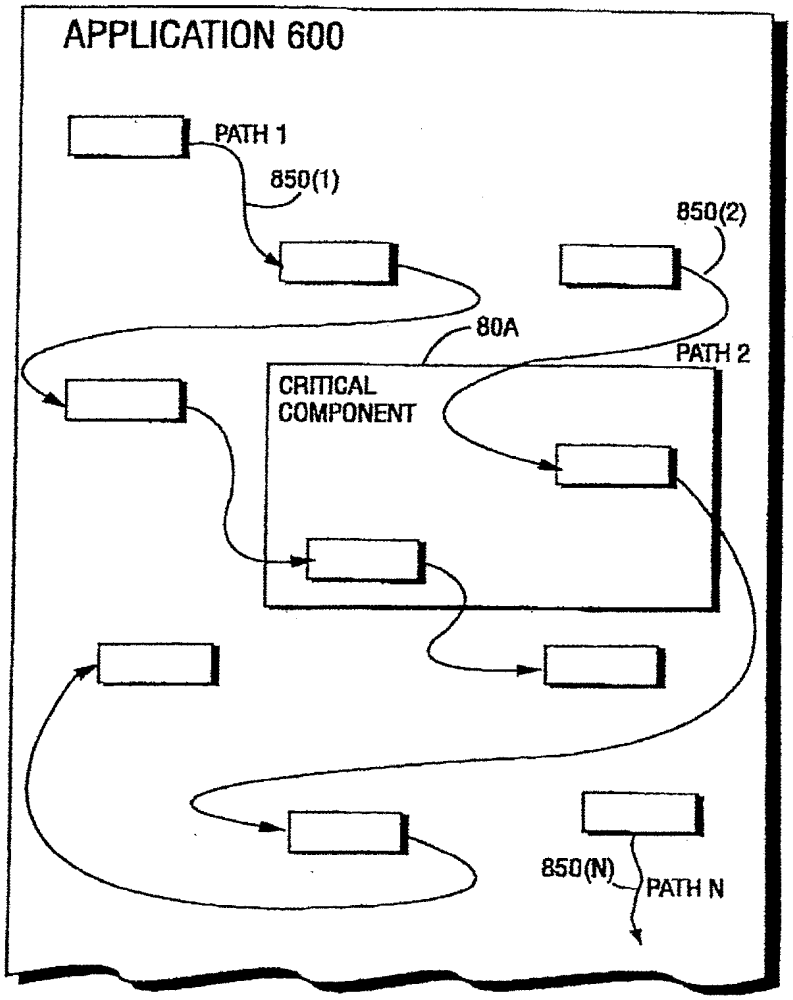


FIG. 20C PSEUDO-RANDOM VALIDATION PATHS IN APPLICATION

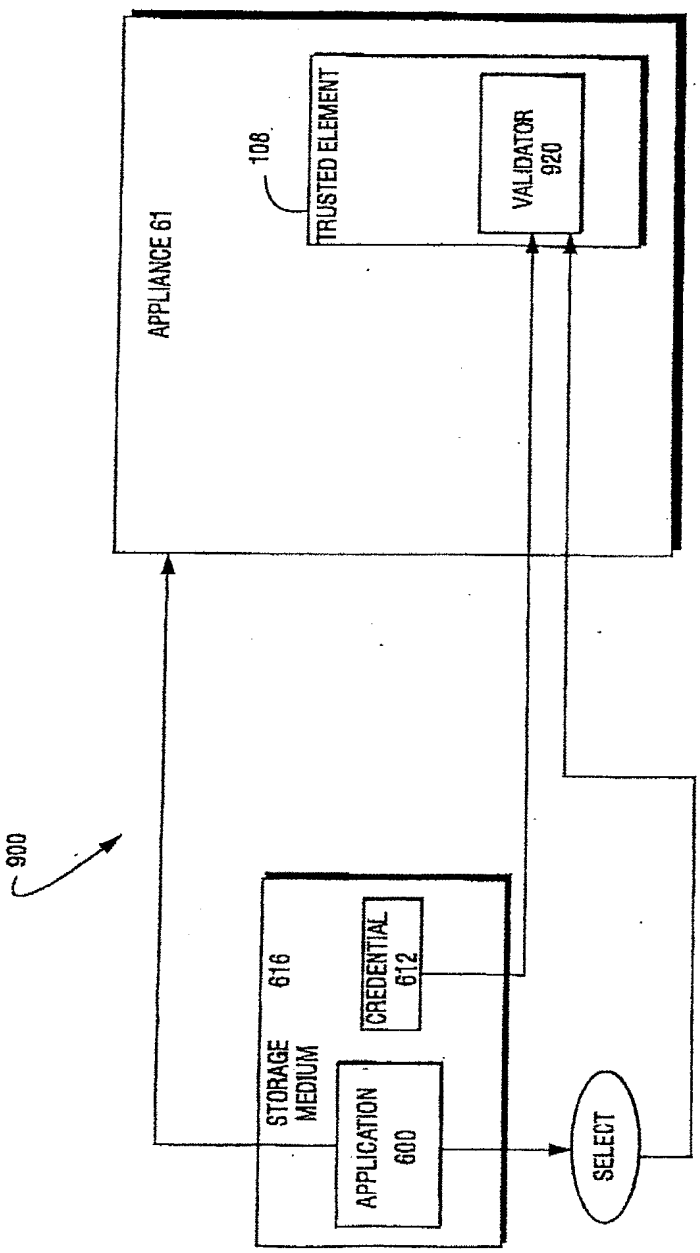
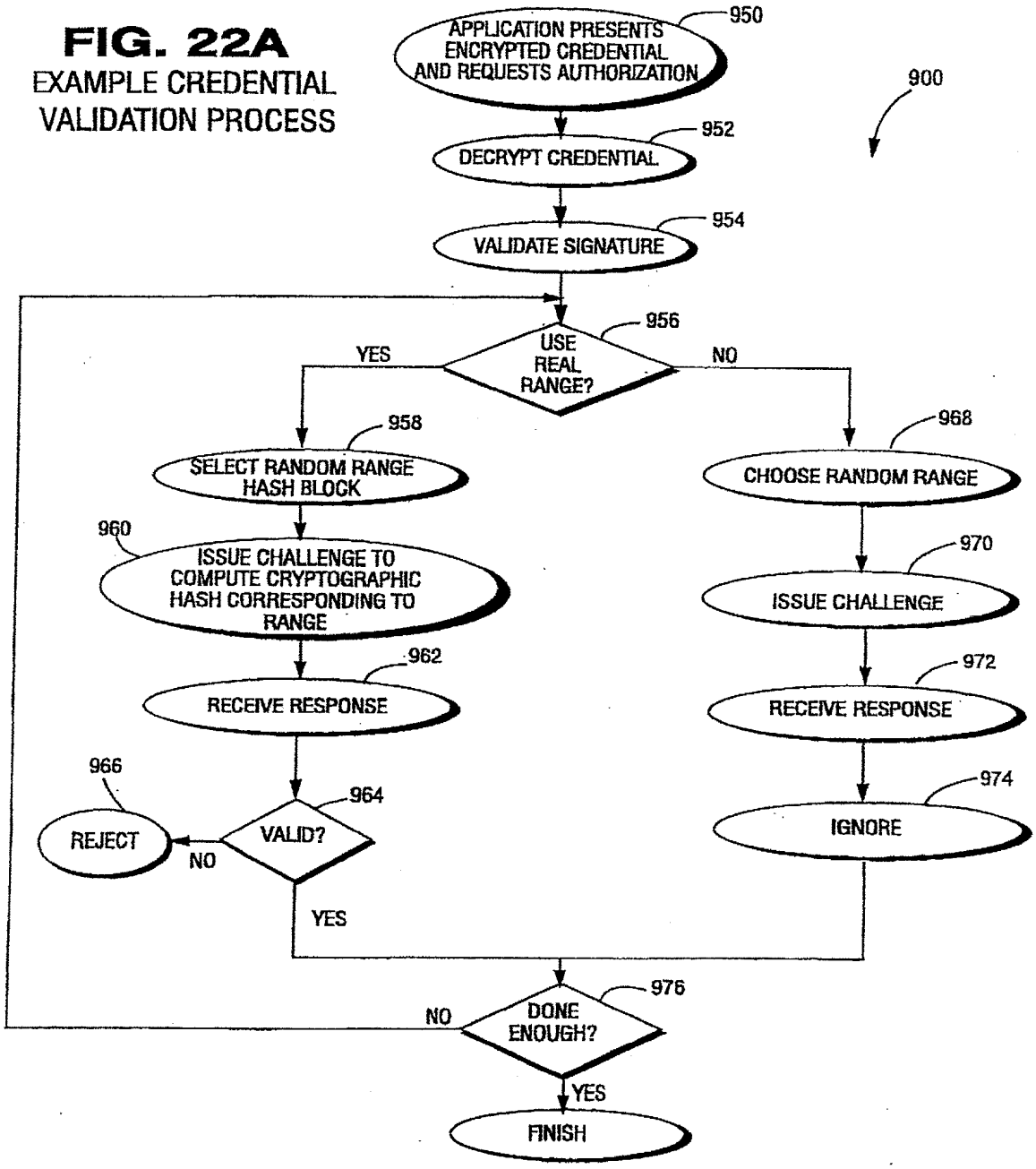


FIG. 21 EXAMPLE CREDENTIAL VALIDATION PROCESS

FIG. 22A
EXAMPLE CREDENTIAL VALIDATION PROCESS



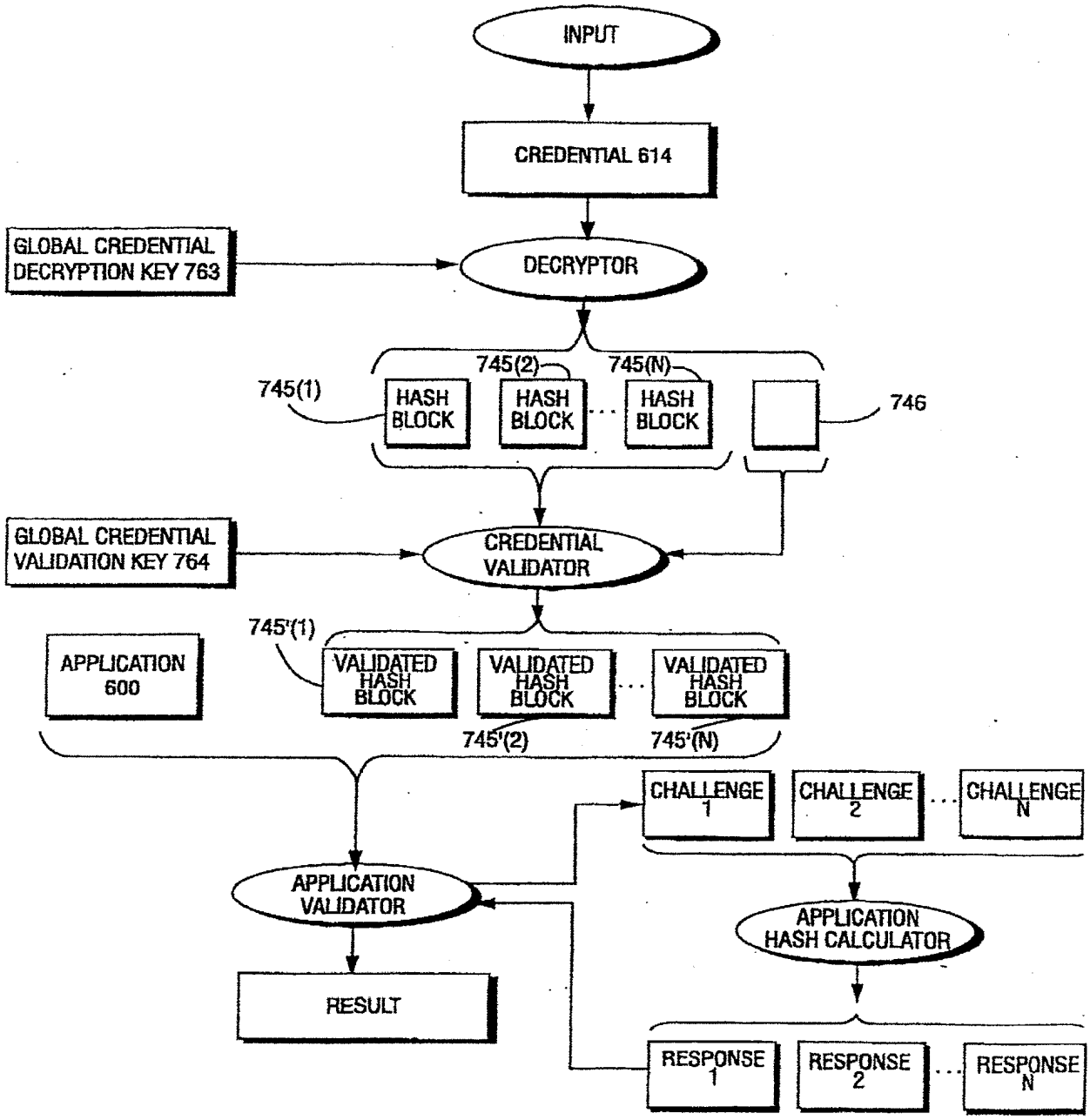


FIG. 22B EXAMPLE CREDENTIAL VALIDATION